Portfolio of Internal & External Affairs Representing the GOVERNMENT OF THE CAYMAN ISLANDS TENDER No: CTC/10-11/PIE/016

REQUEST FOR PROPOSALS for: Immigration Biometric Enrolment, Verification, and Enforcement Hardware and Software, and Law Enforcement Automated Fingerprint Identification System Hardware and Software

Date: 8th October, 2010

TABLE OF CONTENTS

RECEIPT OF TENDER DOCUMENTS 4
SECTION 1: INVITATION TO TENDER 6
Invitation 6
Part A: Immigration Biometric Enrolment, Verification, and Enforcement Hardware and Software 6
Part B: Automated Fingerprint Identification System Hardware and Software. 8
SECTION 2: INSTRUCTIONS TO TENDERERS 10
Government's Representative 10
Tenderer's Submissions 10
Tendering Regulations 13
Notices to Tenderers 14
Government's Policy on Confidentiality. 14
Confidential Information (proprietary information and trade secrets) 15
Further Information and Clarification 16
Amendment to the Tender Document 16
Proposal Prices 16
Validity of Tender 17
Terms of Payment 17
Joint Ventures 17
Conflict Of Interest 18
News Releases 18
Contract Negotiation 18
Notice of Intent to Award - Tenderer Notification of Selection 18
Discussions/Negotiations 19
Errors in Preparation 19
Warranty and Support Services 19
SECTION 3: CONDITIONS OF TENDER 21
Eligibility Criteria 21
Background 23
Statement of Objectives 23
Requirements 24
Detailed Requirements 25
1. Enrolment Equipment & Supporting Software 25
2. Verification Equipment & Supporting Software 28
3. Single Finger Matching Software Development Kit & License 30
4. Fingerprint 1:N Uniqueness Search System & License 32
5. Mobile Fingerprint Capture and 1:1 Matching Device (MFCMD) 37
Section 3 - Part B: Automated Fingerprint Identification System Hardware and Software. 47
Background 47
Statement of Objectives 47
Requirements 48
Detailed Requirements 49
6. Existing RCIPS AFIS Specification 49

7. AFIS Upgrade Requirements 54
8. Requirements – Desktop/Portable Livescan Terminals 57
9. Data Conversion Requirements 61
10. Requirements for Integration with other Systems 62
11. Warranty / Support Requirements 63
12. Training Requirements 63
14. Optional - Mobile AFIS Device Requirements 64
15. Optional – Offsite Disaster Recovery 67
Parts A & B 68
Acceptance Criteria 68
Execution of Contract 68
Project Timetable 68
SECTION 4: ASSESSMENT CRITERIA 70
TENDER PRICE FORM 71

RECEIPT OF TENDER DOCUMENTS

Email to RFPbiometrics@gov.ky

TENDER NO: CTC/10-11/PIE/016

FOR: Procurement of Immigration Biometric Enrolment, Verification, and Enforcement Hardware and Software, and Law Enforcement Automated Fingerprint Identification System Hardware and Software

RECEIVED
BY:

_____

(PRINT Name of Person) FOR AND ON BEHALF OF:

_____

(PRINT Name of Company) Company Street Address:

Company Postal Address: _____

Company Tel &/or Cell: _____

Contact email address: _____

Date and Time Submitted: _____ _____

(Date) (Time)

The Tenderer is advised of the following:

1. The deadline date, time and address for receipt of bid submissions: November 19th, 2010, noon (local Cayman time), by physical delivery of a response document (see Section 1, clause 3 below for delivery details).

2. The format for bid submission is: Five (5) hard paper copies of your proposal including Tender Price Form plus one (1) CD/DVD containing an electronic copy of your proposal and Tender Price Form. The CD/DVD may contain other supporting or background materials or presentations, however only the proposal

and Tender Price Form will be assessed (see Section 4 – Assessment Criteria for details).

3. Late proposals received after the deadline will not be evaluated and will be returned to the Tenderer after the proposal opening meeting.

4. The Cayman Islands Government:
   a. is under no obligation to accept the lowest bid
   b. may award the tender to multiple Tenderers
   c. can cancel a tender process and/or reject all proposals at any time prior to the award of the tender.

SECTION 1: INVITATION TO TENDER
TENDER NO: CTC/10-11/PIE/016

FOR: Procurement of Immigration Biometric Enrolment, Verification, and Enforcement Hardware and Software, and Law Enforcement Automated Fingerprint Identification System Hardware and Software

Invitation

1. The Government of the Cayman Islands acting herein and represented by the Portfolio of Internal & External Affairs ("the Portfolio") invites suitably qualified biometric enrolment and verification equipment, Automated Fingerprint Identification System (AFIS) equipment, and software providers to submit a proposal for Immigration Biometric Enrolment, Verification, and Enforcement Hardware and Software, and Automated Fingerprint Identification System Hardware and Software.

2. The Cayman Islands Government is interested in procuring:

Part A: Immigration Biometric Enrolment, Verification, and Enforcement Hardware and Software

A. Immigration Biometric Enrolment, Verification, and Enforcement Hardware and Software ("the Immigration System"). The Immigration System must:

i. Provide the capability to enrol up to 30,000 persons annually using fixed live scan fingerprint / palm print enrolment devices.

ii. Provide the capability to biometrically verify fingerprints for up to 115,000 persons annually each year using fixed and mobile handheld devices (see Section 3 – Part A for search times and accuracy threshold requirements)

iii. Allow for future growth in the system, including allowing Cayman Islands Department of Immigration satellite offices (in Jamaica. and Honduras) to enrol persons and biometrically verify fingerprints. This

includes providing biometric infrastructure that is extensible in the future as needs change.

iv. Allow for the future interface of the Immigration System with AFIS databases in other jurisdictions (e.g. to facilitate the searching of work permit holder prints against print databases in other jurisdictions, where the Cayman Islands Government has established a memorandum of understanding to control and provide for this interaction.) This includes capturing and storing biometric records in industry standard, widely used, formats.

v. Provide the ability for the Department of Immigration to submit a subject's prints to the RCIPS AFIS system (see Section 3 - Part B) for matching against latent prints taken from crime scenes. This includes capturing and storing biometric records in industry standard, widely used formats that can be communicated to the RCIPS AFIS system.

B. Provide a tool for mobile biometric verification to assist immigration enforcement in the Cayman Islands, with capability to store up to 30,000 fingerprint templates on the mobile devices for real-time response when cellular coverage is not available (see Section 3 – Part A for search times and accuracy threshold requirements)

C. Provide software, Software Developer Kit (SDK) training, and training documentation for up to 10 Cayman Islands Government employees.

D. Provide end-user biometric device usage information material to support preparation of online and poster user help guides for biometric devices deployed for this effort.

E. Provide local warranty and support in Cayman Islands for biometric devices over a minimum 5-year period from contract award.

Part B: Automated Fingerprint Identification System Hardware and Software.

A. Automated Fingerprint Identification System Hardware and Software ("the AFIS System"). The AFIS system must:

   i. Provide an upgraded capability for the Royal Cayman Islands Police Service ("RCIPS") to search finger, palm, and latent prints against a database of criminal print records, and to support integration with the existing RCIPS Cogent Mugshot System (CMS).

   ii. Provide adequate AFIS System capacity to support future growth. Note: it is estimated that the current CAFIS system will reach its current storage capacity limit in 12-24 months.

   iii. Provide a fast, accurate, and reliable AFIS system to support the RCIPS for at least 10-20 years.

   iv. Allow integration and controlled access between the AFIS System and the Immigration System.

   v. Integrate the AFIS and existing CMS to allow better search capabilities, and the near real-time verification of identity.

   vi. Provide the ability for the RCIPS to submit latent prints from crime scenes to the Immigration biometric system (see Part A) for matching against work permit holder biometric records. .

   vii. Provide the ability for the RCIPS to submit a subject's prints to the AFIS for matching against latent prints taken from crime scenes.

   viii. Perform fast, accurate 1:N search capabilities to support timely RCIPS policing operations (see Section 3 – Part B for desired search times and accuracy thresholds).

   ix. Provide a desktop live scan system that can be deployed at RCIPS stations as required.

B. Optionally provide RCIPS with the opportunity to acquire add-on solutions for additional AFIS system functionality, including mobile AFIS devices, and remote off-site disaster recovery for the AFIS and the existing CMS.

C. Provide AFIS System training and training documentation for up to 10 Cayman Islands Government employees.

D. Provide local warranty and support in Cayman Islands for the AFIS System over a minimum 5-year period from contract award.

3. The proposal is to be submitted in physical format to

The Secretary of the Central Tenders Committee
Ground Floor
Government Administration Building
71A Elgin Avenue, George Town
Grand Cayman KY1-9000
Cayman Islands

no later than noon on November 19th, 2010 (local Cayman time).

SECTION 2: INSTRUCTIONS TO TENDERERS

Government's Representative

1. The Government nominates the Deputy Chief Officer of the Portfolio of Internal & External Affairs or any person acting for him (hereinafter called the "Government Representative") as the Government's representative. The Government Representative has appointed an Immigration Biometric Enrolment, Verification, and Enforcement Hardware and Software, and Law Enforcement Automated Fingerprint Identification System Hardware and Software Project Team ("the Project Team") from whom all instructions will be sought including any questions in connection with this Invitation. The Project Team may be contacted by email to: RFPbiometrics@gov.ky. All contact with Government regarding this Tender must go thru this email address. If you have queries concerning this Project, do not call by telephone nor send emails to individual members of the Project Team.

Tenderer's Submissions

2. Any general queries or uncertainties of interpretation arising from the tender documents should be brought to the attention of the Project Team in writing (email) at the earliest opportunity. Queries will only be accepted up to November 8th at noon (local Cayman time).

3. All documents are to be submitted in English. Your proposal should be submitted in detail and accompanied by a completed Tender Price Form (or likeness) included at the end of this Invitation to Tender documentation. Pricing shall be given in Cayman Islands Dollars. Tenderers may choose to respond with pricing for some or all of the requested hardware and software components. The Government reserves the right to award the Tender to multiple Tenderers. The Government reserves the right to give preference to Tenderers who are able to supply all hardware and software components. For Part B, the Government

reserves the right to give preference to Tenderers who reuse existing AFIS infrastructure.

4. All responses, as described, must be fully completed and typed or printed in ink and must be signed in ink with the firm's name and by an officer or employee having authority to bind the company or firm by his/her signature. Proposals having any erasures or corrections must be initialled in ink by person signing the response or the response may be rejected.

5. If so required, the unit price for each unit offered shall be shown, and such price shall include packaging, handling and shipping, any relevant Government duty, export licences, and delivery charges to a Grand Cayman premises, or to Cayman Brac for devices to be used in that location, unless otherwise specified.

6. You are required to keep your proposal confidential and not to divulge to anyone, even approximately, what your proposed price is or will be. The sole exception to this is information you may have to give to your insurance company or broker in order to compile your proposal, but you must stress to them that this information is given in strict confidence.

7. You must not make any arrangements with anyone else about whether or not they should tender, or about their or your tender prices or terms and conditions. You may however, obtain any necessary subcontract quotations.

8. Your proposal must include a cover letter summarizing the firm's interest in the RFP and contain a signature of an individual authorized to legally bind the person, partnership, company, or corporation submitting the proposal.

   The cover letter must also contain the name, street address, telephone number, fax number, web site URL, and e-mail address of the proposing firm. In addition, the cover letter must disclose the Tenderer's legal status: sole proprietor, partnership, corporation, Limited Liability Company, etc.

9. Your form of proposal with all relevant documents should be submitted in a sealed envelope prominently marked "CTC/10-11/PIE/016: Immigration Biometric Enrolment, Verification, and Enforcement Hardware and Software, and Law Enforcement Automated Fingerprint Identification System Hardware and Software". The envelope or package should not bear any indication of the identity of the Proposer.

10. Proposers are advised that at the time of submitting the proposal, the cashier will issue a manual receipt stating the date and time the proposal has been received and the person submitting the proposal shall also sign the receipt, a copy of which is issued to the person submitting the proposal.

11. The person signing the receipt agrees with the date and time the proposal has been submitted and there is no recourse by them or any other person to dispute these facts at a later stage.

12. Although a late proposal may be received by the cashier it will be rejected as a "late bid" during the tender opening process and will be returned to the proposer immediately after the tender opening meeting.

13. If the proposal is qualified it may be set aside as a non-responsive counteroffer, or you may be required to withdraw the qualification without amending your Proposal.

14. Ineligible proposals will be rejected prior to evaluation.

15. The Government:

A. is under no obligation to accept any or the lowest bid

B. shall not defray any cost incurred by Tenderers

C. may award part or all of this tender to different Tenderers

D. may cancel a tender process and/or reject all proposals at any time prior to the award of the tender

E. may waive minor informalities that:

- Do not affect responsiveness;
- Are merely a matter of form or format;
- Do not change the relative standing or otherwise prejudice other offers;
- Do not change the meaning or scope of the RFP;
- Are trivial, negligible, or immaterial in nature;
- Do not reflect a material change in the work; or
- Do not constitute a substantial reservation against a requirement or provision.

F. reserves the right to reject any Tenderer or proposal determined to be non-responsive. The Government also reserves the right to refrain from making an award if it determines that to be in its best interest.

16. Tenderers are advised that although a late proposal may be received it will be rejected as "late" during the proposal opening process and notice sent to the Tenderer immediately after the proposal opening meeting;

Tendering Regulations

17. The process of public procurement is regulated by Part 9 of the Financial Regulations (2004) and subsequent revisions. This Invitation to Tender has been prepared to accord with these Regulations and is subject to all applicable Cayman Islands Laws. This tendering process will be conducted through the Central Tenders Committee.

18. The objective of this invitation is to provide an open and competitive environment, ensuring that the evaluation of tenders is carried out in a fair, ethical, impartial, consistent, transparent manner, with a publicly auditable mechanism, a declared basis for the evaluation of tenders, and with no obligation to accept the lowest price only.

19. Government's procurement process recognises:

A. the overriding requirement to ensure value for money

B. that all proposals are to be evaluated fairly, and impartially against the eligibility and evaluation criteria stated in the advertisement and tender documentation

C. that commercially sensitive information is treated confidentially and in accordance with applicable laws

Notices to Tenderers

20. All Tenderers are advised to complete the attached Receipt of Tender Documents [hereafter called the "Acknowledgement"] and email the completed Acknowledgement to RFPbiometrics@gov.ky as soon as possible.

21. Any subsequent Notice to Tenderers issued by the Project Team will be emailed to those persons or companies that have provided an Acknowledgement.

Government's Policy on Confidentiality.

22. The tender remains the property of the Cayman Islands Government and may be used only to prepare a proposal in response. Except for information to the public generally (other than by breach of these Conditions), a person receiving the tender must not publish, disclose or copy any of its content, except to prepare a proposal in response. The Tenderer must keep confidential all information provided by the Government, as part of, or in connection with, the tender documentation. All proposals become the property of the Cayman Islands Government which may reproduce all or any part for evaluation despite any confidentiality or intellectual property right subsisting in the successful proposal that gives rise to a binding contract with the Government:

23. The Government and the Tenderer must hold the tender in confidence, so far as the law allows, except if:

A. The information is available to the public generally, other than by breach of this obligation a law requires a party to file, record or register something that includes information in the tender

B. disclosure is necessary or advisable to get a consent, authorisation, approval or license from a Governmental or public body or authority

C. it is necessary or advisable to make disclosure to a taxation or fiscal authority

D. it is necessary to provide the information in the tender in answer to a question asked of a Minister in the Legislative Assembly, or otherwise to comply with a Minister' s obligations to the Legislative Assembly

E. it is disclosed confidentially to a party's professional advisors: 1) to get professional advice about this tender process 2) otherwise to consult such professional advisors

Confidential Information (proprietary information and trade secrets)

24. All proposals and other material submitted become the property of the Cayman Islands Government and may be returned only at the Government's option. All proposals and related information, including detailed cost information, will be held in confidence until an award is made.

25. After award, proposals will be subject to the Government's Freedom of Information Law. Records are closed or confidential only if specifically stated in law. Tenderers may make a written request that trade secrets and other proprietary data contained in proposals be held confidential. Material considered confidential by the Tenderer must be clearly identified, and the Tenderer must include a brief statement in their transmittal letter that sets out the statutory basis for confidentiality. The Evaluation Committee will respond to the Tenderer's request, in writing, with a written determination whether the information is an exception to

the Freedom of Information Law, and the information will be processed appropriately.

Further Information and Clarification

26. For further information on the Invitation to Tender please address all correspondence to tender no CTC/10-11/PIE/016 - Immigration Biometric Enrolment, Verification, and Enforcement Hardware and Software, and Law Enforcement Automated Fingerprint Identification System Hardware and Software Project Team via email RFPbiometrics@gov.ky. Please note that queries by telephone are not acceptable.

Amendment to the Tender Document

27. Tenderers should note that the Portfolio may amend the tender documents by issuing an addendum prior to the deadline of the submission of tenders. This may be in response to clarification requested or any omission made by the Project Team. Any such addendum will be sent to the registered prospective Tenderers by email.

Proposal Prices

28. The price(s) stated on the Tender Response Form shall constitute the full compensation payable to the Tenderer for the goods, services and works and shall include, unless otherwise expressly stated, all cost, taxes, duties, fees or charges of any kind whatsoever. All prices shall include packaging, handling and shipping, any relevant Government duty, export licences, and delivery charges to a Grand Cayman premises, or to Cayman Brac for devices to be used in that location, unless otherwise specified.

Validity of Tender

29. Parties tendering are expected to state the period for which the proposal is valid. This period must be at least 120 days after the proposal submission date of this RFP.

Terms of Payment

30. Payment is contingent upon successful completion of Project deliverables, and will be made upon receipt of an invoice from the Tenderer for those completed and approved deliverables. The payment schedule will be finalized during contract negotiations. The final negotiated cost will not be exceeded. It is understood that after receipt of an invoice, the Cayman Islands Government will require up to thirty (30) days to process the invoice for payment.

31. No claim for additional services, not specifically provided herein, will be allowed by the Government except to the extent provided by a valid modification or amendment to this agreement.

Joint Ventures

32. Joint ventures will not be allowed in response to this procurement. For the purposes of this procurement, a joint venture is defined as follows:

A risk sharing partnership arrangement of two (2) or more Tenderers, who have teamed together to address a Project's set of contracted services. In this type of partnership, no single Tenderer assumes the lead role of "prime contractor" over one or more partner "subcontractors".

However, the use of subcontractors by the successful Tenderer is allowed, as long as the successful Tenderer is the sole prime contractor. Planned involvement or actual use of subcontractors on this Project must be approved by the Government of the Cayman Islands in writing before any involvement of the subcontractor in Project activities. If subcontractors are approved, the successful Tenderer to this RFP will be the sole point of contact for all efforts on this Project.

Conflict Of Interest

33. Tenderers must disclose any instances where the firm or any individuals working on the contract has a possible conflict of interest and, if so, the nature of that conflict. The Government of the Cayman Islands reserves the right to cancel the award if any interest disclosed from any source could either give the appearance of a conflict or cause speculation as to the objectivity of the Tenderer's proposal. The CI Governments' determination regarding any questions of conflict of interest will be final.

News Releases

34. News releases related to the contracts awarded from this RFP may only be made with prior approval of the Government of the Cayman Islands.

Contract Negotiation

35. After final evaluation, the Evaluation Committee may negotiate with the Tenderer of the highest-ranked proposal. Negotiations, if held, will be within the scope of the request for proposals and limited to those items that would not have an effect on the ranking of proposals. If the highest-ranked Tenderer fails to provide necessary information for negotiations in a timely manner, or fails to negotiate in good faith, the Government may terminate negotiations and negotiate with the Tenderer of the next highest-ranked proposal. When contract negotiations are held, the Tenderer will be responsible for all cost including its travel and per diem expenses.

Notice of Intent to Award - Tenderer Notification of Selection

36. After the completion of contract negotiation, the Evaluation Committee will issue a written Notice of Intent to Award and send copies to all Tenderers. The Notice of Intent Award will set out the names and addresses of all Tenderers and identify the proposal selected for award. The scores and placement of other Tenderers will not be part of the Notice of Intent to Award.

The successful Tenderer named in the Notice of Intent to Award is advised not to begin work, purchase materials, or enter into subcontracts relating to the Project until both the successful Tenderer and the Government sign the contract.

Discussions/Negotiations

37. By submission of a response to this solicitation, the Tenderer agrees that during the period following issuance of the solicitation and prior to the final award of contract, the Tenderer will not discuss this procurement with any party, other than its subcontractors if applicable.

Errors in Preparation

38. The Proposal Evaluation Committee has the right to rely on cost proposal provided by Tenderers. The Tenderer may be responsible for any mathematical error or incorrect extension of any calculations leading to Tenderer's cost proposal. The Proposal Evaluation Committee reserves the right to reject proposals that contain errors.

Warranty and Support Services

39. Notwithstanding prior acceptance by the Government of the Cayman Islands of any deliverables under any contract resulting from this RFP, the Tenderer expressly warrants all documentation, reports, and other items as correct and complete with the terms of the contract.

Upon recognition of an error, deficiency or defect on behalf of the Tenderer, the Government will notify the Tenderer in writing citing the specific deficiency. The Tenderer will, within ten (10) days of receipt of such notice, respond with a plan to correct any deficiencies cited in correspondence. If the plan is inadequate to correct the deficiency, or if the Tenderer fails to implement the plan, or to correct the error, deficiency or defect, or the error recurs, the Government may, at its

option, act to correct the problem. The Tenderer will be required to reimburse the Government within 30 days for any such costs incurred or the Government may consider this to be cause for breach of contract.

End of Section 2: Instructions to Tenderers.

SECTION 3: CONDITIONS OF TENDER

Eligibility Criteria

The Tenderer's response shall include the submission of relevant and verifiable data and references providing evidence that the vendor and its personnel, available either in-house or outsourced, is suitably qualified.

The Tenderer's response will demonstrate that the company has the relevant experience providing the services and goods for which they are submitting a proposal, and that any staff proposed for positions on this Project has the appropriate knowledge and experience obtained on Projects of similar nature, size, and scope. The Cayman Islands Government may require substitution/replacement of any key personnel assigned to the Project if it determines that person does not possess the skills necessary to satisfactorily complete the tasks assigned.

To demonstrate qualifications, the Tenderer's proposal must provide the following:

- Company Experience
  The Tenderer must possess a verifiable past record of providing the proposed equipment and/or software to a local, state, or national government entity that is equal to or supersedes the Project's size and complexity. Proposals must provide a statement explaining corporate and staff knowledge in the specific areas on which the company is submitting a proposal. Experience preferably will be from the last five years, although earlier experience may be submitted if it demonstrates continuity of services over a broad span of years.
- Related Experience
  Proposals must describe similar Projects, completed or currently in process, within the past five years that demonstrate the skills and services to be used in this Project. The proposal should include a description of the history of each Tenderer Project. Additionally, the Tenderer will provide the following information related to three previous and/or current contracts, which are considered identical or similar to the requirements of this RFP:
    - Name, address, and telephone number of contracting agency;

- The name of the contracting agency Project director who may be contacted for verification of all information submitted. If the Project director is not available as a reference, a suitable substitute and a statement of justification may be included;
- Contracts with government agencies;
- Dates of the contracts; and
- A brief, written description of the specific prior services performed and the outcome of that engagement.

- Personnel/Staff Experience

  Proposals must provide an assurance that the Tenderer has the staff to produce the Project deliverables. The Tenderer will provide an organizational chart and staffing plan of the individuals proposed to work on this Project.

- Legal Claims / Judgements

  Proposals must provide details of any claims, judgments, arbitration proceedings or suits pending or outstanding against your company, its officers, any employee or any supplier, individual or corporate, to be engaged by you for the Project, arising from the procurement of your goods during the last five (5) years.

Section 3 - Part A: Immigration Biometric Enrolment, Verification, and Enforcement Hardware and Software

Background

The Cayman Islands Department of Immigration ("the Department") manages the growth of the Cayman Island's population by regulating the flow of immigrants into the islands and carries out administrative processing of applications for persons seeking permanent residence, Caymanian status, the right to work in Cayman, or asylum. The Department is empowered by the Immigration Law to take and retain the biometric information of work permit holders. The Department is contained within the Portfolio of Internal and External Affairs of the Cayman Islands Government ("the Portfolio").

The Head of the Department is the Chief Immigration officer who reports to the relevant officer of the Portfolio. The Portfolio is responsible to the Deputy Governor, who in turn reports to His Excellency The Governor who is appointed by the United Kingdom.

The Portfolio is physically located at the Government Administration building in George Town, Cayman Islands. The Department has offices on Grand Cayman and Cayman Brac, including its primary headquarters in George Town, at the District Administration Building on Cayman Brac, as well as immigration processing facilities at Owen Roberts International Airport in Grand Cayman ("GCM"), at Gerrard Smith International Airport on Cayman Brac ("CYB"), and at the Cayman Islands Port in George Town

Statement of Objectives

The purpose of the project is to integrate a biometric identity verification capability with the existing Cayman Islands Immigration Support Services (IMSS) Java application, developed by the Cayman Islands Government Computer Services Division (CSD). This will be accomplished via the procurement and integration (by CSD) with IMSS of five biometric components as defined in the Detailed Requirements section of this document. These five components will provide the hardware and software to biometrically enrol and verify the identities of work permit holders and their dependents living in Cayman Islands.

Enrolments will be performed at fixed locations in office environments and will include capture of ten rolled and flat fingerprints and full palm images. The enrolment process will include a 1:N fingerprint uniqueness search that ensures each individual's biometrics are associated with a single identity in IMSS. In addition the enrolment process may include a search of the Cayman Islands Police AFIS system to determine if the permit holder has been found guilty of a disqualifying offense (see Part B of this document for a description of the current AFIS system). Permit holder identities will be biometrically verified using both fixed and mobile devices. Fixed verification units will be deployed at selected points of entry and will operate in typical office environments. Mobile verification devices must operate in outdoor conditions and be able to interoperate with a back-end database system or as a stand-alone system if back-end communications are not available.

Tenderers must offer Software Development Kits (SDKs) that support integration of their devices and biometric applications with existing Immigration Department applications. SDKs must include documentation explaining their use, and Tenderers are also required to provide support for CSD personnel performing integration, including for the provision of a fixed number of phone support hours.

Requirements

The Portfolio and Department desire to procure Immigration Biometric Enrolment, Verification, and Enforcement Hardware and Software. Our required features and functionalities are explained in the Detailed Requirements section of this document. The below table outlines the expected quantities of each hardware component required. Adequate software licenses should also be priced to allow for the use of these devices given the detailed requirements below.

The Cayman Islands Government will provide or purchase server hardware based on the specifications that are provided for the core application software and the interfaces. Server and operating system costs should be excluded from your proposal.

Quantities of Biometric Devices and Licences Required			
	Enrolment (Palm Prints / 10 Prints)	**Fixed 1:1 Verification Devices**	**Mobile Enforcement Devices**
Immigration HQ	4	2	
GCM Airport	2	15	1
GAT (General Aviation Terminal – at GCM)	1	1	
Cayman Seaport		1	2
CYB Airport	1	2	2
Mobile Enforcement		2	10
Total Operational Devices	**8**	**23**	**15**
Spares	1	3	4
CSD Development Support	1	1	1
Total Devices	**10**	**27**	**20**

Detailed Requirements

The Fingerprint, Palm Enrolment Equipment, and Supporting Software will be used by CSD to integrate a biometric enrolment and verification capability with the existing IMSS Java application. The following five Hardware and Software components are requested to be priced by Tenderers. The Tenderer's response should address their capability to meet all requirements. Tenderers may choose to respond with pricing for some or all of the requested hardware and software components. The Government reserves the right to give preference to Tenderers who are able to supply all hardware and software components.

1. **Enrolment Equipment & Supporting Software**

   The enrolment process will capture ten rolled fingerprint images, three flat slaps, (two of which will each consist of four flat finger images from the left and right hands with the third consisting of two flat images of the thumbs) and left and right palm prints.

The equipment will be used in office environments with controlled climate conditions.

1.1 Functional Requirements

1.1.1 The fingerprint & palm capture equipment shall be FBI Appendix F compliant.

1.1.2 The equipment shall be capable of capturing rolled fingerprint images.

1.1.3 The equipment shall be capable of capturing flat slap images, in which all four fingers of one hand or both thumbs are captured simultaneously.

1.1.4 The equipment shall be capable of capturing palm prints, including the entire palm print (including the writer's palms and the sides of the palms).

1.2 Environmental / Physical Requirements

1.2.1 The minimum platen size shall be 1.6 in x 1.5 in (Rolled), 3.2 in x 2.0 in (Slaps), and 4.9 in x 4.9 in (Palms).

1.2.2 The minimum image resolution captured by the equipment shall be 500 dpi.

1.2.3 The equipment shall be capable of operating in temperatures ranging from 35 to 100 degrees Fahrenheit, and relative humidity ranging from 10 to 90%, non-condensing.

1.2.4 The equipment shall have a Mean Time Between Failures of at least 4,160 hours.

1.2.5 Equipment shall be compatible with 120 VAC, 60 Hz electrical power.

1.3 Warranty / Support Requirements

1.3.1 Equipment shall be delivered with a minimum of a one-year warranty for all defects not caused by abuse. Warranty term shall begin upon acceptance.

1.3.2 The Tenderer shall provide detailed pricing for hardware and software maintenance for each year of the four years following the warranty period.

1.3.3 Tenderer shall include a minimum of 60 hours of phone support in their offer. Phone support shall include an initial overview session, with the

remainder of hours available for as-needed use. Phone support hours shall be billed based on the actual usage of hours by the Government.

1.4 Hardware Requirements

1.4.1 The equipment shall connect to a workstation using a USB interface, and shall include all cables and external power supplies necessary for connection and use.

1.4.2 Tenderers must include user manual(s) providing maintenance and operating procedures.

1.5 Software Requirements

1.5.1 Drivers and supporting software must be capable of running under both Windows 2000 and Windows XP Professional, with Windows 7 support (in addition to Windows XP Professional) preferred

1.5.2 Software must be capable of returning images in lossless Windows Bit Map (BMP) format.

1.5.3 Tenderers must include a software development kit (SDK) suitable for integrating the equipment with an existing Java application (IMSS).

1.5.4 The SDK must include a user guide for integration with Java application.

1.5.5 The SDK must correctly set all fields in BMP DIB header.

Table 1.1 Palm Print / Ten Print Enrolment Capture Device Specs

Image Quality	FBI IQS IAFIS Image Quality Specification Appendix F
Scanner Interface	USB 2.0 or higher, or FireWire A IEEE 1394
Power Requirements	120 VAC / 60 Hz
Reliability	MTBF at least 4,160 hrs
Temperature	35-100 degrees F
Humidity	10%-90%, non-condensing
Platen Size	1.6 in x 1.5 in (Rolled), 3.2 in x 2.0 in (Slaps), 4.9 in x 4.9 in (Palms)
Warranty / Support	Min. 1 year, 5-yr support via maintenance plan or fee-for-service plan.
OS Requirements	Windows 2000, XP Pro, or Windows 7-compatible
Additional Software Requirements	Require SDK to integrate solution with Java applications

2. Verification Equipment & Supporting Software

The Fingerprint Verification Equipment & Supporting Software will be used at fixed points of entry to capture fingerprint images for biometric verification of the identities of work permit holders and their dependents. This equipment will be used in a temperature & humidity controlled environment.

2.1 Functional Requirements

2.1.1 The fingerprint verification equipment shall be capable of capturing one or two flat fingerprint impressions

2.2 Environmental / Physical Requirements

2.2.1 The minimum platen size shall be 0.5 inches wide by 0.7 inches high (1-finger) or 1.6 inches wide by 1.5 inches high (2-finger).

2.2.2 The minimum image resolution captured by the equipment shall be 500 dpi.

2.2.3 The equipment shall be capable of operating in temperatures ranging from 35 to 100 degrees Fahrenheit, and relative humidity ranging from 10 to 90%, non-condensing.

2.2.4 The equipment shall have a Mean Time Between Failures of at least 4,160 hours.

2.2.5 Equipment shall be compatible with 120 VAC, 60 Hz electrical power.

2.3 Warranty / Support Requirements

2.3.1 Equipment shall be delivered with a minimum of a one-year warranty for all defects not caused by abuse. Warranty term shall begin upon acceptance.

2.3.2 The Tenderer shall provide detailed pricing for hardware and software maintenance for each year of the four years following the warranty period.

2.3.3 Tenderer shall include a minimum of 60 hours of phone support in their offer. Phone support shall include an initial overview session, with the remainder of hours available for as-needed use. Phone support hours shall be billed based on the actual usage of hours by the Government.

2.4 Hardware Requirements

2.4.1 The equipment shall connect to a workstation via a USB interface.

2.4.2 The bid must include user manual(s) providing maintenance and operating procedures.

2.5 Software Requirements

2.5.1 Drivers and supporting software for the equipment must be capable of running under both Windows 2000 and Windows XP Professional, with Windows 7 support (in addition to Windows XP Professional) preferred

2.5.2 Software must be capable of returning images in lossless Windows Bit Map (BMP) format.

2.5.3 The bid must include a software development kit (SDK) suitable for integrating the equipment with a Java application.

2.5.4 The SDK must include a user guide for integration with Java applications.

2.5.5 If equipment captures more than one fingerprint at a time, SDK must support image segmentation to create separate BMP files containing each individual fingerprint.

2.5.6 SDK must correctly set all fields in BMP DIB header.

Table 2.1 Fingerprint Verification Device Specs

Image Resolution	Min. 500 dpi
Scanner Interface	USB 2.0 or higher
Power Requirements	120 VAC / 60 Hz
Reliability	MTBF at least 4,160 hrs
Temperature	35-100 degrees F
Humidity	10%-90%, non-condensing
Platen Size	0.5 in x 0.7 in (1-finger), or 1.6 in x 1.5 in (2-finger)
Warranty / Support	Min. 1 year, 5-yr support via maintenance plan or fee-for-service plan.

3. Single Finger Matching Software Development Kit & License

The Single Finger Matching Software Development Kit & License shall provide the ability for CSD to integrate a fingerprint matching capability with the Immigration Support Services (IMSS) Java application. It will be used to compare single-finger images to fingerprints captured during the biometric enrolment process for the purpose of verifying the identity of work permit holders and their dependents.

3.1 Functional Software Requirements

3.1.1 The SDK must support integration with Java applications.

3.1.2 The SDK must convert single fingerprint images in standard Windows BMP format to ANSI INCITS 378-2009 "Information Technology – Fingerprint Minutiae Format for Data Interchange" templates.

3.1.3 Templates generated by the SDK may use the Extended Data area of the template to enhance matching results; however, data in the mandatory data area must comply with the standard in all respects and be consumable by other compliant fingerprint matchers.

3.1.4 The SDK may optionally include the ability to incorporate multiple fingerprint views into a single template.

3.1.5 The SDK shall not reject or refuse to create a template for any submitted fingerprint image.

3.1.6 The SDK shall return one or more fingerprint quality metric(s) in response to each template generation request.

3.1.7 Each fingerprint quality metric shall be predictive, in that it is strongly correlated with fingerprint matching success.

3.1.8 The Tenderer shall provide metrics, preferably generated via third-party testing, that demonstrate the predictive ability of the offered quality metric(s). The Tenderer shall clearly identify the source of this data, including contact information for third party testers and links to test results if applicable.

3.1.9 The SDK shall provide the ability to compare two ANSI INCITS 378-2009 compliant templates.

3.1.10 The SDK shall allow the calling application to set the matching threshold.

3.1.11 The Tenderer shall provide information, preferably generated via third-party testing, which specifies the False Match Rate and False Non-Match Rate corresponding to matching threshold settings. The Tenderer shall clearly identify the source of this data, including contact information for third party testers and links to test results if applicable.

3.1.12 The SDK shall return a matching result based on the specified matching threshold to the calling application.

3.1.13 The SDK may optionally include the ability to compare a single fingerprint view in one template to multiple minutiae views in the other template ("multi-view capability"). This feature may return a single matching score or an array of matching scores containing one score for each view compared.

3.1.14 If the SDK includes a "multi-view" capability, it shall include the ability to update an existing template with one or more additional views without regenerating the entire template.

3.1.15 The SDK shall include documentation that fully explains SDK features, use and integration with Java applications.

3.1.16 A copy of SDK documentation shall be included with the Tenderer's proposal.

3.1.17 The Tenderer shall provide detailed pricing for the use of the template generator and matcher in their proposal. Pricing shall be based on the number of systems on which the software is installed, and shall not depend on the number of persons enrolled, number of templates generated or number of matches performed.

3.1.18 The Tenderer shall provide license costs for the Single Finger matching software, including a unit price schedule for additional licences.

3.1.18.1 Licences shall be transferable across users or desktops without additional charge.

3.2 Warranty / Support Requirements

3.2.1 The Tenderer shall warranty the SDK, template generator and matcher for a period of one year. Defects shall be corrected during this period at no additional cost.

3.2.2 The Tenderer shall provide detailed pricing for software maintenance for each year of the four years following the warranty period.

3.2.3 Tenderer shall include a minimum of 120 hours of phone support in their offer. Phone support shall include an initial overview session, with the remainder of hours available for as-needed use. Phone support hours shall be billed based on the actual usage of hours by the Government.

4. Fingerprint 1:N Uniqueness Search System & License

The Fingerprint 1:N Uniqueness Search System & License will provide the Cayman Islands Computer Systems Division with a toolset needed to integrate a uniqueness search with the Immigration Support Services (IMSS) application. This search will be used in conjunction with the enrolment capability to ensure that each work permit holder or dependent has only one IMSS identity associated with their fingerprints.

This capability may also be used to perform 1:N ten print searches of fingerprints captured by other systems.

4.1 Functional Software Requirements

4.1.1 The 1:N search system shall initially support up to 115,000 identities

4.1.2 The 1:N search system shall be expandable to 500,000 identities by adding server(s) and purchasing licenses for the desired capacity.

4.1.3 The 1:N search system shall perform searches using ten print flat fingerprints.

4.1.4 The 1:N search system shall accommodate search requests in which fingers cannot be printed due to bandages or amputation without diminishing the accuracy achieved when ten prints are available.

4.1.5 The 1:N search system shall have a configurable matching threshold.

4.1.6 The 1:N search system shall provide support for review of matching ten prints.

4.1.6.1 When a match occurs, the 1:N search system shall return the unique identifiers associated with the matching identities to the calling application.

4.1.6.2 The 1:N search system shall provide a mechanism for the calling application to retrieve the fingerprint images associated with the matching identities.

4.1.6.2.1 Providing the ability to retrieve the images associated with a unique identifier is an acceptable method of meeting this requirement.

4.1.7 The 1:N search system shall allow all 1:N search system functions to be accessed from a Java application (e.g., via web service call).

4.1.7.1 The Tenderer shall provide details of the interfaces provided.

4.1.8 The 1:N search system shall provide a "search & add" transaction in which a search is performed and if no match is found, a new identity is added to the system.

4.1.8.1 Providing separate 'Search' and 'Add' transactions for use by the calling application is an acceptable method of meeting this requirement.

4.1.9 The 1:N search system shall provide a "Search Without Add" transaction that performs a search but does not add the identity to the system if no match is found.

4.1.10 The Tenderer shall provide 1:N search system documentation explaining the system's use, maintenance, log file interpretation, troubleshooting and Application Programming Interface(s) used to access its features.

4.1.10.1 The documentation shall include the data format required for search submissions.

4.1.10.2 The documentation shall include a software installation and configuration guide that provides step-by-step instructions for initial installation and configuration, as well as for adding

additional server(s) to accommodate growth in the number of enrolled persons.

4.1.10.3 A current version of this documentation shall be submitted as part of the Tenderer's proposal.

4.1.11 The Tenderer shall provide information, preferably generated via third-party testing, which specifies the False Match Rate and False Non-Match Rate corresponding to matching threshold settings. The Tenderer shall clearly identify the source of this data, including contact information for third party testers and links to test results if applicable.

4.1.12 The Tenderer shall provide recommended server configurations for the 1:N fingerprint search software.

4.1.12.1 Each configuration shall be designed to process a minimum of 60 searches per hour with a maximum search time of 1 minute per search.

4.1.12.2 Configurations in which a workflow management server is used to coordinate the activities of matching servers may specify a different configuration for the workflow management server.

4.1.12.3 The 1:N search system shall have the ability to automatically continue to operate without loss of functionality in the event of the failure of a single matching server.

4.1.12.3.1 The Tenderer shall quantify the performance degradation resulting from failure of a single matching server, including the time required for system reconfiguration.

4.1.12.3.2 The 1:N search system shall notify system operator(s) of matching server failures.

4.1.12.4 Tenderer-provided server configurations shall include but not be limited to:

4.1.12.4.1 Number of processors required per server

4.1.12.4.2 Front Side Bus clock rate required

4.1.12.4.3 Processor clock rate required

4.1.12.4.4 RAM required

4.1.12.4.5 Disk space required

4.1.12.4.6 Operating system required

4.1.12.4.7 Number of servers required for the specified initial number of identities

4.1.12.4.8 The number of servers recommended versus number of identities enrolled, up to 500,000 identities.

4.1.13 The Tenderer shall specify any other software required for use of the 1:N search system but not included in the proposal.

4.1.13.1 Specifications for server(s) and storage required to support any such software shall be included in the Tenderer's proposal. It is acceptable for this server configuration to differ from that recommended for matching and workflow servers.

4.1.14 The Tenderer shall specify the 1:N search system start-up time (i.e., time between operating system start-up and search system readiness for use). The Tenderer shall specify how this time changes with the number of identities enrolled. Times specified shall assume the use of the recommended server configuration(s) and quantities.

4.1.15 The Tenderer's proposal shall specify the 1:N search times for a database containing various numbers of enrolled identities when using the recommended hardware configuration.

4.1.15.1 Search times shall be specified using the example table shown below.

4.1.15.2 Times shall be based on the assumption that the Tenderer's recommended hardware configuration will be used for each number of identities.

4.1.15.3 If search time varies for transactions in which a new identity is added to the system versus those in which no identity is added, both times shall be specified.

Table 4.1 Search Time Performance

Number of Identities in System	System Search Time with Add	System Search Time with no Add
500		
1,000		
5,000		
10,000		
25,000		
50,000		
100,000		
150,000		
200,000		
250,000		
300,000		
350,000		
400,000		
450,000		
500,000		

4.1.16 The 1:N search system shall provide the ability to associate each identity added with a unique number specified by the calling application.

4.1.17 The 1:N search system shall provide the ability for the calling application to remove an identity from the 1:N search database, with the identity to be deleted specified using the unique number associated with the identity.

4.1.18 When an identity is removed from the 1:N search database, all templates and images associated with the identity shall be permanently deleted.

4.1.19 The 1:N search system shall retain fingerprint images when adding an identity to its database.

4.1.20 The 1:N search system shall link retained fingerprint images to the associated identity.

4.1.21 The Tenderer shall provide license costs for the 1:N search system.

4.1.21.1 Unless otherwise specified in Tenderer's proposal, licenses shall be assumed to be based solely on the number of enrolled identities.

4.1.21.2 Licenses shall be transferable across servers without additional charge.

4.1.21.3 If license cost varies depending on the number of identities stored in the system, license costs shall be provided for the following numbers of identities.

Table 4.2 Identity license costs

Number of Identities	License Cost
50,000	
100,000	
150,000	
115,000	
200,000	
250,000	
300,000	
350,000	
400,000	
450,000	
500,000	

4.2 Warranty / Support Requirements

4.2.1 The Tenderer shall warranty the 1:N search system for a period of one year. Defects shall be corrected during this period at no additional cost.

4.2.2 The Tenderer shall provide detailed pricing for software maintenance for each year of the four years following the warranty period.

4.2.3 Tenderer shall include a minimum of 120 hours of phone support in their offer. Phone support shall include an initial overview session, with the remainder of hours available for as-needed use. Phone support hours shall be billed based on the actual usage of hours by the Government.

5. Mobile Fingerprint Capture and 1:1 Matching Device (MFCMD)

The purpose of the MFCMD is to provide Cayman Islands Immigration Enforcement with a mobile ability to verify the identity of work permit holders using 1:1 fingerprint matching. Immigration Enforcement officers will enter the first name, last name and date of birth of the person being verified into the MFCMD to establish the claimed identity of a putative work permit holder. The MFCMD will capture one or more flat fingerprints, which will be compared to the biometric data captured from the permit holder during enrolment, and return a match result, match confidence

score, facial image, work permit status and immigration status of the work permit holder. MFCMD requirements can be satisfied by Tenderers with one of two different types of devices.

The first type is a mobile capture device with an integrated computer capable of wirelessly sending fingerprint(s) and demographic data to a back-end server that identifies the associated claimed identity, matches fingerprint(s) and returns results, statuses, and facial image(s). The device must be capable of displaying the data received from the back-end server. This device must also be capable of storing and matching captured fingerprints against specific fingerprint templates in a locally-stored database. The device must display a match result, match confidence score, facial image, work permit status and immigration status of the work permit holder. The device will be used in this mode in the event that the MFCMD cannot communicate with the back-end server for any reason. In the remainder of this section, this type of device will be referred to as a "*mobile verification device*". Provision must be made for synchronizing the local device database with the IMSS back-end database in a secure fashion.

The second type of compliant MFCMD is a fingerprint capture device that interoperates with a laptop computer to provide the same functionality as the mobile verification device. Cayman Islands Immigration Enforcement has existing laptop computers in their vehicles that can be used to store records and perform local searches when the MFCMD cannot communicate with the back-end server for any reason. In the remainder of this section, this type of device will be referred to as a "*mobile capture device*".

Except as noted, the following requirements apply to either type of MFCMD.

5.1 Functional Requirements

5.1.1 The Mobile Fingerprint Capture and 1:1 Matching Device (MFCMD) shall be capable of capturing two fingerprints (two separate single-finger captures is an acceptable means of meeting this requirement)

5.1.2 The MFCMD shall store captured fingerprint(s) as standard Windows Bit Map (BMP) images.

5.1.3 The MFCMD shall have the ability to communicate securely with other computers using wireless communication technology.

5.1.4 The MFCMD shall be capable of capturing fingerprint images with a minimum resolution of 500 dpi.

5.1.5 The MFCMD shall be capable of capturing fingerprint images with a minimum size of 250 pixels wide by 350 pixels high.

5.1.6 The MFCMD shall be designed for hand-held use, such that the device can be held by an immigration officer while a work permit holder's fingerprints are captured.

5.1.7 The MFCMD shall perform one or more biometric quality assessments on captured fingerprint image(s) and prompt for recapture of images of insufficient quality.

5.2 Environmental / Physical Requirements

5.2.1 The MFCMD shall be capable of operating for at least 8 hours on a single battery charge.

5.2.2 The MFCMD battery shall not degrade in performance if recharged before being fully discharged.

5.2.3 The MFCMD shall support hot-swap of batteries; i.e., it must be possible to change batteries in the middle of an operation without loss of data.

5.2.4 Each MFCMD shall be provided with charger(s) that allow at least two batteries to be charged concurrently.

5.2.5 MFCMD chargers must be compatible with 120 VAC, 60 Hz electrical power.

5.2.6 MFCMD shall be capable of being powered by standard automobile power outlets, either through a dedicated charger or the use of an inverter. Dedicated chargers or compatible inverters, if required, shall be included in the price of the units.

5.2.7 The MFCMD shall be capable of operating in temperatures ranging from 35 to 120 degrees Fahrenheit, and relative humidity ranging from 10 to 90%, non-condensing.

5.2.8 The MFCMD shall be water resistant; it shall not fail when exposed to rain, or to brief immersion in water.

5.2.9 The MFCMD fingerprint scanner shall operate in direct sunlight or shade.

5.2.10 The MFCMD shall weigh no more than 4 pounds.

5.2.11 The MFCMD shall have an external carry case or other protective container to prevent damage during transit.

5.2.12 The MFCMD shall be capable of sustaining a fall of 4 feet or less without damage.

5.2.12.1 Tenderer shall discuss in their tender their device's ability to survive such falls without damage.

5.3 Warranty / Support Requirements

5.3.1 The MFCMD shall be delivered with a minimum of a one-year warranty for all defects not caused by abuse. Warranty term shall begin upon acceptance.

5.3.2 The MFCMD shall have a Mean Time Between Failures of at least 4,160 hours.

5.3.3 The Tenderer shall provide detailed pricing for hardware and software maintenance for each year of the four years following the warranty period.

5.3.4 Tenderer shall include a minimum of 60 hours of phone support in their offer. Phone support shall include an initial overview session, with the remainder of hours available for as-needed use. Phone support hours shall be billed based on the actual usage of hours by the Government.

5.4 Mobile Verification Device - Specific Requirements

The following requirements apply only to the mobile verification device, if this approach is taken by the Tenderer. The Tenderer shall provide software that runs on the Mobile Verification Device that includes the following capabilities, or

alternately provide a Software Development Kit that allows the following capabilities to be developed

5.4.1 The device shall capture the subject's first name, last name and date of birth via manual data entry. The device may have the ability to capture this information from an existing passport document, or magnetic strip ID card, in additional to manual entry.

5.4.2 The device shall support one or more of the following wireless communication protocols:

5.4.2.1 A cellular communications protocol (e.g. GPRS/EDGE) offered by providers in the Cayman Islands (e.g. a local cellular company such as LIME or Digicel). This requirement can be met by providing a device that does not have internal cellular support but can access cellular communications by operating with a RIM BlackBerry device in tethered mode. Tenderers shall provide details of supported device(s) (including required device software revision levels) and any third party software required.

5.4.2.2 Wi-Fi (802.11g or higher)

5.4.3 The device shall support TCP/IP communication, either via wired Ethernet (100 Mbps or higher) or secure Wi-Fi (802.11g or higher).

5.4.4 The device shall have the ability to encrypt data transmissions to protect against interception using industry standard encryption.

5.4.4.1 The Tenderer shall specify the encryption algorithm and key size used by their device.

5.4.4.2 The Tenderer shall not propose proprietary encryption schemes.

5.4.5 The device shall have the ability to securely transmit the subject's two fingerprint images, first name, last name and date of birth to the back end system.

5.4.6 The device shall have the ability to confirm successful receipt of transmissions by the back-end system, and to retransmit in the event of transmission failure.

5.4.7 The device shall have the ability to securely receive and decrypt a response consisting of the work permit holder's name, date of birth, work permit and immigration status and facial image, and to display this information to the immigration enforcement officer.

5.4.8 The device shall have the ability to submit additional verification requests while previous requests are processed by the back-end system.

5.4.9 The device shall have the ability to list previously submitted transactions for which no response has been received.

5.4.10 The device shall have the ability to query previously submitted search requests in the event that the device was turned off or out of communication with the back-end system when the response was transmitted.

5.4.11 The device shall have the ability to internally store a repository of up to 30,000 work permit holder and dependent data records.

5.4.11.1 These records shall include the work permit holder's (or dependent's) first name, last name, date of birth, at least two fingerprint images or templates, facial image, work permit status and immigration status.

5.4.11.1.1 It is estimated that each record will consume approximately 13 KB, assuming that each fingerprint template requires 1K, facial image requires 10K and names, date of birth and statuses require 1K of storage.

5.4.11.2 The device shall protect the internal repository from unauthorized access.

5.4.11.2.1 Tenderer shall explain in detail how the internal repository is protected on their device. The use of encryption for this purpose is preferred.

5.4.12 The device shall have the ability to synchronize the internal repository with the immigration database by processing 'add', 'change' and 'delete' commands issued by the immigration database.

5.4.12.1 Each device shall have a unique identifier that allows IMSS to track synchronization status by device.

5.4.12.2 These features shall be accessible by Java applications.

5.4.13 In the event that verification queries cannot be sent to the back-end system (e.g., if the device is outside of the cellular service area), the device shall have the ability to search the local repository.

5.4.13.1 The device shall use the first name, last name and date of birth to display a list of candidate matches to the immigration enforcement officer.

5.4.13.2 The device shall allow the immigration enforcement officer to select the matching record and initiate verification of the captured fingerprint images against those of the work permit holder in the local repository.

5.4.13.3 The device shall the retrieve the subject's name, date of birth, work permit and immigration status and facial image, and to display this information to the immigration enforcement officer.

5.4.13.4 The device shall complete local verification requests in no more than 10 seconds.

5.4.13.5 When operating in this "local" mode, the device can complete each search before initiating the next.

5.4.14 The Tenderer shall provide costs for the Mobile Verification device, including matching software, system software, communications software, and any other required licences. The Tenderer shall also include a unit price schedule for additional licences.

5.4.14.1 Unless otherwise specified in Tenderer's proposal, licenses shall be assumed to be based solely on the number of mobile units purchased.

5.4.14.2 Licenses shall be transferable between Mobile Verification devices without additional charge.

In contrast to the mobile verification device discussed above, the mobile capture device will use the immigration enforcement laptop as an intermediary for communication with the back-end system, as well as for local searches. Tenderers proposing a mobile capture device must also offer either a software suite, or a Software Development Kit (SDK) that allows Cayman Islands Computer Systems Division to integrate the mobile capture device with immigration enforcement laptops.

Typical configuration for the existing Cayman Islands Immigration Enforcement laptops is provided below.

Table 5.1 Fingerprint Verification Device Specs

Configuration Item	**Configuration**
Processor Model	AMD Turion 64 mobile technology ML-37 2 GHz
Processor Clock Rate	2 GHz
Random Access Memory	1 GB – 2Gb standard
Disk Space	60 GB standard
Network Ports	10/100/1000
Operating System	32bit Windows XP SP3
Wireless Communication Device(s)	IEEE 802.11b, IEEE 802.11a, IEEE 802.11g GPRS/EDGE connectivity for field deployment, with apps accessed via Citrix with RSA authentication

5.5 Mobile Capture Device - Specific Requirements

The following requirements apply only to the mobile capture device, if this approach is taken by the Tenderer.

5.5.1 The device shall support Wi-Fi (802.11g or higher).

5.5.2 The device shall be capable of transmitting two fingerprint images to an immigration enforcement laptop.

5.5.3 The Tenderer shall provide software that runs on the immigration enforcement laptop that includes the following capabilities, or alternately

provide a Software Development Kit that allows the following capabilities to be developed:

5.5.3.1 The software shall have the ability to encrypt data transmissions to protect against interception using industry-standard encryption algorithm and key sizes.

5.5.3.2 The software shall have the ability to securely transmit the subject's two fingerprint images, first name, last name and date of birth to the back end system.

5.5.3.3 The software shall have the ability to confirm successful receipt of transmissions by the back-end system, and to retransmit in the event of transmission failure.

5.5.3.4 The software shall have the ability to securely receive and decrypt a response consisting of the work permit holder's name, date of birth, work permit and immigration status and facial image, and to display this information to the immigration enforcement officer.

5.5.3.5 The software shall have the ability to submit additional verification requests while previous requests are processed by the back-end system.

5.5.3.6 The software shall have the ability to query previously submitted search requests in the event that the software was turned off or out of communication with the back-end system when the response was transmitted.

5.5.3.7 The software shall have the ability to internally store and search a repository of up to 30,000 work permit holder and dependent data records.

5.5.3.7.1 These records shall include the work permit holder's (or dependent's) first name, last name, date of birth, at least two fingerprint images or templates, facial image, work permit status and immigration status.

5.5.3.8 The software shall have the ability to synchronize the internal repository with the immigration database by processing 'add',

'change' and 'delete' commands issued by the immigration database.

5.5.3.9 These features shall be accessible by Windows applications developed using Microsoft Visual Studio 2007.

5.5.3.10 In the event that verification queries cannot be sent to the back-end system (e.g., if the laptop is outside of the cellular service area), the software shall have the ability to search the local repository.

5.5.3.10.1 The software shall use the first name, last name and date of birth to display a list of candidate matches to the immigration enforcement officer.

5.5.3.11 The software shall allow the immigration enforcement officer to select the matching record and initiate verification of the captured fingerprint images against those of the work permit holder in the local repository.

5.5.3.12 The software shall retrieve the subject's name, date of birth, work permit and immigration status and facial image, and display this information to the immigration enforcement officer.

5.5.3.13 The software shall complete local verification requests in no more than 10 seconds.

5.5.3.14 When operating in this "local" mode, the device can complete each search before initiating the next.

5.5.4 The Tenderer shall provide costs for the Mobile Capture device, including matching software, system software, communications software, and any other required licences. The Tenderer shall also include a unit price schedule for additional licences.

5.5.4.1 Unless otherwise specified in Tenderer's proposal, licenses shall be assumed to be based solely on the number of units purchased.

5.5.4.2 Licenses shall be transferable between without additional charge.

Section 3 - Part B: Automated Fingerprint Identification System Hardware and Software.

Background

The Royal Cayman Islands Police Service (RCIPS) is the primary law enforcement agency in the Cayman Islands. It serves all three of the Cayman Islands (Grand Cayman, Cayman Brac and Little Cayman.) Together they comprise approximately 101 square miles of land. The service is made up of approximately 350 police and auxiliary officers, supported by approximately 60 police support staff and a team of Special Constables. The RCIPS has seven physical stations, including George Town (Central Police Station), West Bay, East End, North Side, Bodden Town, Cayman Brac, and Little Cayman. Further background information on the RCIPS is available on the RCIPS website at http://www.rcips.ky/.

Statement of Objectives

The purpose of this solicitation is to provide an upgraded capability for the RCIPS to search fingerprints against a database of criminal fingerprint records and support integration with the existing RCIPS Cogent Mugshot System (CMS). Additionally the RCIPS seeks a solution that supports integration with the new Immigration identity tracking capability. The Automated Fingerprint Identification System (AFIS) will need to have the capabilities to support Ten-print vs. Ten-print search (TPTP), latent print versus ten-print (LTTP), ten-print versus unsolved latent print (TPUL), Palm print versus Palm print (PPPP) and Latent Palm versus Palm print (LPPP). This capability will need to support accuracy response times and throughput defined in table 2. Additionally, the RCIPS requires a limited number of booking stations and a support environment for operations.

RCIPS encourages the Tenderer to provide responses that meet the noted requirements with novel approaches that reduce cost.

Requirements

The Portfolio of Internal and External Affairs (the Portfolio) and the RCIPS desire to update the currently installed AFIS system, first installed in 2003. The purpose of this update is to ensure that the RCIPS has access to a fast, accurate, and reliable AFIS system, with sufficient storage capacity to meet future needs, as well as to integrate the existing CMS with AFIS to allow real time identity verification. In addition, the Portfolio and the RCIPS wish to further expand the use of the AFIS system, including its integration with the Department of Immigration's Work Permit Biometric system to allow controlled inter-system searching of both civilian work permit and criminal biometric records. This Request for Proposal (RFP) is being run in conjunction with the Immigration Work Permit Biometric System RFP, to ensure that supplied systems are interoperable.

Tenderer's can propose the update of the AFIS system either as an upgrade or a replacement of the existing system. Tenderer's may reuse existing AFIS and CMS hardware and software components in their proposal, where appropriate, to reduce the project cost and implementation effort. Preference may be given to Tenderers who adopt a reuse strategy. Additionally, Tenderers can propose alternate procurement models where the RCIPS does not own the equipment.

The below table outlines the expected quantities of each component required. Adequate software licenses should also be priced to allow for the use of these devices given the detailed requirements below. Server hardware and operating system costs should be included with the proposal.

Quantities of Devices and Licences Required (minimum) *** Note: The quantities below may be reduced if the Tenderer re-uses existing hardware, software, or licence components. Further quantities may be required to provide adequate redundancy. The Tender may include other hardware devices or licences as their proposed solution requires.**	
AFIS Server	1 (there is 1 currently in place available for reuse)
AFIS Workstations and User Licences	3 (there are 3 currently in place available for reuse)
Livescan Booking Workstations	2 (there are 2 currently in place available for reuse)
Desktop Livescan Workstations	3 (currently none in place)
Mobile AFIS Devices (Optional)	4 (currently none in place)
Total Items	***13***

Detailed Requirements

The RCIPS AFIS System Hardware and Software project will upgrade or replace the existing RCIPS AFIS system. The Tenderer's response should address their capability to meet all upgrade requirements listed below as well as provide the same or similar functionality to the existing AFIS environment, with similar or better performance metrics.

6. Existing RCIPS AFIS Specification

6.1 System Architecture and Hardware/Software Specification

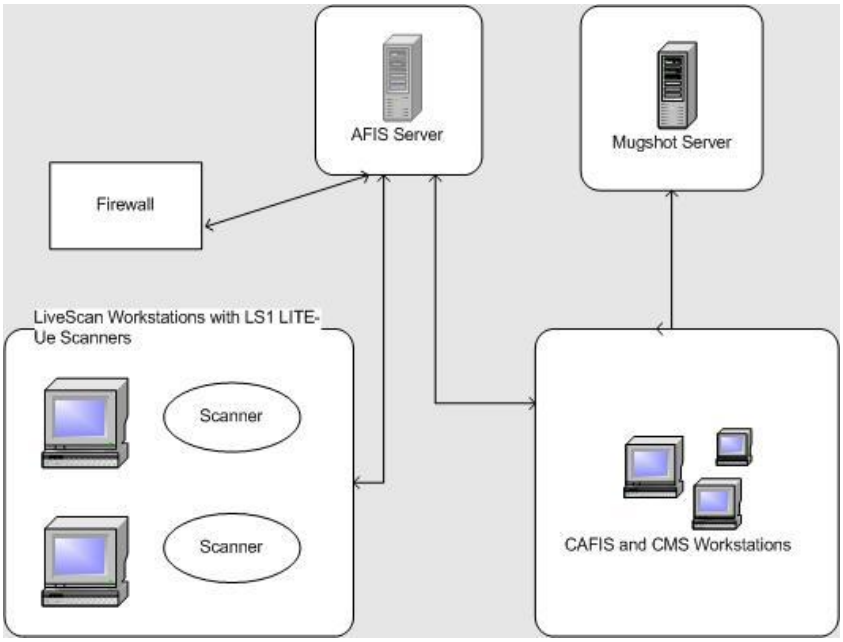
6.1.1 The current RCIPS AFIS system uses the following hardware and software:

- Cogent CAFIS version 5.1 AFIS system;
- Cogent Mugshot System (CMS) version 3.0;
- Three (3) Cogent CAFIS/CMS client desktop workstations;
- Two (2) Cogent Livescan workstations (cabinet configuration) for law enforcement booking operations, each with a Cogent LS1 LITE-Ue scanner;
- A Nikon USB connected video system for capturing latent prints; and
- Ancillary devices, including Xerox Phaser 4500 laser printers to enable printing, and network devices (e.g. switches, etc.)

6.1.2 All devices are connected on a private internal network within the RCIPS, and are protected from the general RCIPS internal network with a firewall device.

6.1.3 The CMS is accessible via a web browser over the internal RCIPS network, including from select terminals outside of the private internal network.

6.1.4 The below diagram provides a high-level depiction of the current AFIS and CMS solution.



6.1.5 The Livescan workstation systems are installed in two (2) physical locations, being the RCIPS Central Police station in George Town, and the West Bay Police station, both on Grand Cayman. One of these stations was purchased and installed in 2003, with the other purchased and installed in 2010.

6.1.6 All CAFIS and CMS workstations run Windows 2000 or Windows XP. Standard configuration includes Pentium 4 2.66 GHZ processors, and at least 512 MB of RAM.

6.1.7 The current AFIS server runs the Windows Server 2003 operating system. It is an IBM eServer xSeries 226 tower. It has a Xeon 3.0 GHZ processor, 2GB of RAM, and 70 GB of storage in a RAID configuration.

6.1.8 The current CMS server runs the Windows Server 2003 operating system. It is an IBM x3200 M2 server.

6.1.9 Oracle is used as the current AFIS server database.

6.1.10 The current AFIS and CMS servers are free-standing tower based servers stored on desks in the Fingerprinting Office at the George Town Central Police station.

6.1.11 The Fingerprinting Office is a standard office environment, using the building's air-conditioning system for environmental control.

6.2 Functional Specification

6.2.1 The RCIPS currently utilises CAFIS for fingerprint and palm print searching and verification.

6.2.2 There are approximately 18,000 (eighteen thousand) records stored in the current CAFIS system.

6.2.3 New records are added either directly through the enrolment of a subject's biometric data through the Livescan workstations, or scanning in of physical fingerprint cards taken at RCIPS stations (stations other than George Town and West Bay) or by Department of Immigration Enforcement officers. Approximately 90% of new records are added through the Livescan workstations.

6.2.4 Latent prints may be obtained from other jurisdictions on an infrequent basis and imported into the system for searches. These latent prints may be received in a variety of electronic formats (e.g. BMP or JPEG images), or physical cards.

6.2.5 The current CAFIS system captures rolled impressions, flat impressions, palm prints, and writer's palms, and is a composite system.

6.2.6 The CMS is used for capturing photos of subjects and basic subject data such as name, date of birth, and other characteristics

6.2.7 Approximately three hundred (300) print verifications are processed by the RCIPS monthly.

6.2.8 Approximately one hundred and fifty (150) latent print searches are processed monthly.

6.2.9 Approximately twenty (20) latent prints are currently added (at a maximum) daily.

6.2.10 Livescan workstations have local storage of records, which are then uploaded to the CAFIS server. The Livescan workstation local database information is deleted periodically.

6.2.11 The current CAFIS system allows the searching of current records by different characteristics (name, demographic, etc.).

6.2.12 The current CAFIS system is used for searching and verification during normal business working hours (Monday to Friday 8.30am – 4.30pm Cayman local time).

6.2.13 The Livescan workstations are used 24/7 to enter subject data (e.g. during booking).

6.3 Performance Specification

6.3.1 The following performance is obtained from the current CAFIS system:

6.3.1.1 Palm print 1:N search results are available in approximately 2 minutes on average.

6.3.1.2 Fingerprint 1:N search results are available in approximately 1 minute on average.

6.3.1.3 Latent 1:N search results are available in approximate 2 minutes on average.

6.3.1.4 Latent Palm 1:N search results are available in approximately 2 minutes on average.

6.4 Operational and Security Specification

6.4.1 The current CAFIS and CMS systems are secured using the built-in application password based security system, as well as physical security controls on the equipment housed at RCIPS locations.

6.4.2 The current CAFIS and CMS systems are administrated primarily by one full time RCIPS fingerprint examiner, with a second RCIPS operator as backup.

6.4.3 Crime scene detectives are given controlled access to the CMS as required.

6.4.4 The Livescan workstations used to enrol subjects to the AFIS and CMS systems are given limited access to CAFIS (e.g. ability to add records only).

6.4.5 All existing hardware and software is owned by the RCIPS.

6.4.6 The current CAFIS vendor is provided with remote access to the system to provide support. However, all vendor staff must be explicitly cleared by the RCIPS prior to access. Access logs are required.

6.4.7 System backups are stored automatically on an external USB hard drive, and removed offsite as required.

6.5 Integration with other Systems

6.5.1 The current CAFIS and CMS systems are not integrated. Neither system can be used to directly access or reference data held by the other.

6.5.2 There are no current direct electronic interfaces with any other system (e.g. Police Booking System, Prison management system, etc.)

6.5.3 There are no current direct electronic interfaces with any other jurisdictions, or with other AFIS systems.

6.6 Support Specification

6.6.1 The current CAFIS maintenance vendor provides a general system helpdesk on a 24/7 basis.

6.6.2 The current CAFIS maintenance vendor provides detailed technical support during normal business hours.

6.6.3 The current CAFIS maintenance vendor has remote access to the CAFIS and CMS systems to provide support.

6.6.4 The current CAFIS maintenance vendor provides onsite support as required.

7. AFIS Upgrade Requirements

7.1 Purpose

7.1.1 The primary purposes of the RCIPS AFIS System Hardware and Software project are to:

- Ensure adequate capacity with the AFIS system to support future growth. It is estimated that the current CAFIS system will reach its current storage capacity limit in 12-24 months.
- Provide a fast, accurate, and reliable AFIS system to support the RCIPS for at least 10-20 years at the current rate with an acceleration rate of 5% per year in repository size and transaction rate.
- Allow integration between the AFIS system and the Department of Immigration's Work Permit Biometric system.
- Integrate the AFIS and the existing CMS to allow better search capabilities, and the near real-time verification of identity.
- Provide a desktop live scan system that can be deployed at RCIPS stations as required.

1.1.2 In addition the project provides the RCIPS with the opportunity to identify potential add-on solutions for additional functionality, including mobile AFIS devices, and remote off-site disaster recovery for the AFIS and CMS systems.

7.2 Project Requirements

7.2.1 Tenderer shall provide technology and implementation details, and detailed pricing for the supply of the hardware, software, and supporting services requested in this RFP.

7.2.2 Tenderer shall provide training, warranty and ongoing support on the terms described below in Warranty / Support Requirements section.

7.2.3 Tenderer shall complete the project including installation and required training within the first quarter of the 2011 calendar year, and provide an implementation timeline in their proposal.

7.2.4 Tenderer shall outline in their proposal how their proposed AFIS upgrade or replacement process will prevent or minimise downtime to the AFIS system (i.e. how RCIPS's normal AFIS operations will be supported during the upgrade or replacement process).

7.2.5 Tenderer shall reuse existing hardware and software in the existing solution, where appropriate, to reduce implementation time and cost.

7.3 AFIS Functional Requirements

7.3.1 Tenderer shall propose a solution that complies with all major industry standards including NIST, and US FBI Appendix F.

7.3.2 The solution shall be capable of providing the same functionality and performance as currently in the existing AFIS system.

7.3.3 The solution shall be integrated with the existing CMS to enable real-time verification of identity, as well as searching of biometric data by search criteria such as subject name, birth date, or other date captured in the CMS.

7.3.4 The integrated solution shall support access via web browser or mobile AFIS device to retrieve CMS mugshot and demographic data information based on the submission of prints (e.g. to link captured prints to the mugshot photo and other demographic information in the CMS). One use case for this, for example, would be a RCIPS officer retrieving mugshot and demographic information in near real-time for a subject based on that

subject's finger print being submitted via an AFIS mobile device and a previous record being returned.

7.3.5 Rates of records stored and being added, searches per hour and number of prints and latent impression are expected to be the same as for the existing system.

7.3.6 The following search function requirements should be met:

7.3.6.1 1:1 print searching for verification of individuals;

7.3.6.2 1:N print searching for comparison against the existing database;

7.3.6.3 1:N searches of newly added prints against unsolved latent prints; and

7.3.6.4 1:N searches of newly added latent prints against the unsolved latent file (to determine if crimes may be linked to the same individual(s)).

7.3.7 On screen viewing shall support third level details (e.g. small shapes on the ridge (edgeoscopy), including ridge unit thickness, thinness and relative pore location).

7.3.8 High quality output is required for printing.

7.3.9 Export requirements include both electronic and paper copies.

7.3.10 Import/Latent Function Requirements include:

7.3.10.1 Import from physical print cards;

7.3.10.2 Support for digital camera import; and

7.3.10.3 The ability to scale and manipulate imported data.

7.3.11 Side by side comparison and ability to print output is required for records.

7.3.12 The Tenderer's solution shall have reporting functionality including the ability to report on system usage, performance, and statistics (e.g. number of processed items, number of processed cases, number of unsolved latent prints, etc.).

7.3.13 If license cost varies depending on the number of records stored in the system, license costs shall be provided for up to 200,000 records.

7.4 Hardware Requirements – AFIS Server, AFIS Workstations, Livescan Booking Workstations

7.4.1 The Tenderer shall provide all hardware required for the solution, and state which of the current hardware is being reused, if any.

7.4.2 New hardware should be based on industry standard technologies. HP or IBM based server and workstation hardware is preferred.

7.4.3 The Tenderer shall include in their pricing any additional hardware required to provide appropriate resiliency and protection against environmental and physical hazards. This shall include redundant power supplies, Uninterruptable Power System (UPS), and a floor-based lockable half-size computer rack if hardware is rack-mounted.

7.4.4 Hardware will operate in a standard office environment (e.g. not in an environmentally controlled server room). Hardware should be capable of operating in temperatures between 60 to 90 degrees Fahrenheit, and relative humidity of between 40 and 75%.

8. Requirements – Desktop/Portable Livescan Terminals

The Tenderer will propose on the supply of desktop/portable Livescan terminal devices, including the Livescan unit and attached laptop terminal, to allow the capture of rolled impressions, flat impressions, palm prints, and writer's palms. The equipment will be used in remote RCIPS office environments with controlled climate conditions.

8.1 Functional Requirements

8.1.1 The fingerprint and palm capture equipment shall be United States Government's FBI Appendix F compliant.

8.1.2 All capture equipment shall provide operator feedback indicating the quality of those prints with clear designation of the need to recapture low quality prints that are below a preset level that is a configuration item controlled in the system maintenance.

8.1.3 The equipment shall be capable of capturing rolled fingerprint images with built-in handling of unprintable or amputated fingers.

8.1.4 The equipment shall be capable of capturing flat slap images, in which all four fingers of one hand or both thumbs are captured simultaneously.

8.1.5 The equipment shall be capable of capturing palm prints, including the entire palm print (including the writer's palms and the sides of the palms).

8.1.6 The equipment shall be United States Government's Rehabilitation Act Amendments (Section 508) compliant.

8.1.7 The equipment shall have a mechanism to capture prints from persons in wheelchairs or with disabilities.

8.1.8 At the time of capture the system shall have the ability to relate fingerprints and palm prints with mugshots taken during the booking process.

8.1.9 Optionally, the equipment may have camera features to allow the taking of subject mugshots, interfacing directly with the existing CMS system. Tenderers proposing this option must explain their capabilities to provide this functionality, as well as technical specifications for the camera system and how it would interface with the existing CMS system.

8.2 Environmental / Physical Requirements

8.2.1 The minimum platen size shall be 1.6 in x 1.5 in (Rolled), 3.2 in x 2.0 in (Slaps), and 4.9 in x 4.9 in (Palms).

8.2.2 The equipment shall be capable of capturing both 500 and 1000 ppi resolution images.

8.2.3 The equipment shall be capable of operating in temperatures ranging from 35 to 100 degrees Fahrenheit, and relative humidity ranging from 10 to 90%, non-condensing.

8.2.4 The equipment shall have a Mean Time Between Failures (MTBF) of at least 4,160 hours.

8.2.5 Equipment shall be compatible with 120 VAC, 60 Hz electrical power.

8.3 Hardware Requirements

8.3.1 Tenderers must include user manual(s) providing maintenance and operating procedures.

Table 8.1 Minimum Desktop Livescan Device Specifications

Image Quality	FBI IQS IAFIS Image Quality Specification Appendix F
Power Requirements	120 VAC / 60 Hz
Reliability	MTBF at least 4,160 hrs
Temperature	35-100 degrees F
Humidity	10%-90%, non-condensing
Platen Size	1.6 in x 1.5 in (Rolled), 3.2 in x 2.0 in (Slaps), 5 in x 5 in (Palms)
Warranty / Support	Min. 1 year, 5-yr support via maintenance plan or fee-for-service plan.
Terminal Laptop	Industry standard laptop connected directly to the Livescan device to allow the RCIPS operator to perform Livescan activities. Preference is for a HP brand laptop. The terminal should include a minimum 15 inch display, and appropriate CPU, RAM and disk space to achieve the performance requirements of the AFIS system.
OS Requirements	Support for XP Professional, and Windows 7

8.4 Performance Requirements

8.4.1 Performance shall meet or exceed the existing AFIS system capabilities.

8.4.2 The proposed solution shall enable the enrolment of an individual into the AFIS system by a trained operator in 5 minutes of less. Enrolment will include scanning of palms combined with roll finger impressions and the capturing of mugshots.

8.4.3 The expected lifetime record volume for the AFIS system is 200,000 records.

8.4.4 The required system accuracy for searches and verification is at least 99.9%. Tenderers shall provide evidence in their proposal of their proposed solution's accuracy, including evidence of a third party accuracy assessment.

8.4.5 The system shall demonstrate the performance from Table 8.2 below for all transaction-types concurrently using data provided by or approved by

the RCIPS in a system that is consistent with the proposed solution. Any difference between the demonstration system and the proposed system must be described and explained.

Table 8.2: Minimum Performance

Index	Search	Minimum Accuracy	Throughput	Repository	Response Time
1	TPTP 1:N	99.9%	60 per hour	200,000 TPF 5000 ULF	1 minute
2	TPTP 1:1	99.99%	120 per hour	200,000 TPF 5000 ULF	30 seconds
3	LTTP	65%	5 per hour	200,000 TPF 5000 ULF	20 minutes
4	TPUL	50%	5 per hour	200,000 TPF 5000 ULF	20 minutes
5	PPPP 1:N	99.9%	6 per hour	200,000 TPF 5000 ULF	10 minutes
6	LPPP	65%	1 per hour	200,000 TPF 5000 ULF	60 minutes

All LTTP and LPPP searches shall be cold searches with no descriptive data. The Unsolved Latent File will be evaluated as a combination of latent palm prints and latent fingerprints.

8.5 Technical Requirements

8.5.1 Windows server-based solutions are preferred for server components.

8.5.2 The desktop solution should be compatible with Windows 2000 and XP currently, with Vista and Windows 7 compatibility highly desirable.

8.5.3 The Tenderer's solution shall provide the ability to perform a complete backup of all records in the AFIS system, including a process to verify that backup has been successfully completed.

8.5.4 The Tenderer's solution shall provide the ability to perform a complete restore from backup of all records in the AFIS system, including a process to verify that restore has been successfully completed.

8.5.5 The Tenderer's solution shall support appropriate security safeguards to ensure the confidentiality, integrity, and availability of the AFIS system, including at a minimum username and password protection, data encryption using industry standard encryption technologies, and support for audit trails within the system.

8.5.6 The Tenderer's solution shall allow for system redundancy, and to the extent possible, avoid single points of failure. The Tenderer shall price adequate hardware to support redundancy.

9. Data Conversion Requirements

9.1.1 The Tenderer shall be responsible for the migration of all existing fingerprint information from the existing system into the proposed solution available at the start of the performance period.

9.1.2 The Tenderer's proposal shall outline an approach to this migration, which may include either re-scanning of all existing print cards, transfer of electronic records from the existing system, or a combination thereof.

9.1.3 The current AFIS system records have 500 ppi resolution, however new records will be captured at 1000 ppi.

9.1.4 In addition to the re-scanning of existing cards, manual or automated entry on names and other data from the cards may be required (e.g. subject name, date of birth, record number, etc). Information on the cards may be printed or handwritten. The cards may be physically up to 20 years old.

9.1.5 The total number of existing physical records is not less than eighteen thousand (18,000) and at time of award will be less than twenty five thousand (25,000).

9.1.6 The existing print cards are of various physical dimensions, including primarily legal and letter size forms.

9.1.7 The Tenderer's solution shall support capture of fingerprint cards at both 500 ppi and 1000 ppi.

10. Requirements for Integration with other Systems

10.1.1 The Tenderer shall provide integration between the AFIS system and the existing CMS.

10.1.2 The integration of the AFIS system and the existing CMS shall allow either system to reference and access the other systems data, to allow real-time verification of subjects.

10.1.3 The Tenderer shall provide a solution that can provide for integration between the RCIPS AFIS system and the Department of Immigration's Work Permit Biometrics system, to enable bi-directional searching to be performed (e.g. allowing prints in one system to be searched for in the other).

10.1.4 Should the Tenderer propose a single combined system for the Immigration System (Part A of this Tender) and AFIS System (Part B of this Tender), the Tenderer shall describe how the proposed solution supports data and administrative separation (e.g. to prevent the mixing of criminal and civil records) and shall propose a solution for access rights management to allow the RCIPS to administrate criminal records, and the Department of Immigration to separately administrate immigration work permit biometric records.

10.1.5 The Tenderer shall provide information on their proposed solution's ability to integrate, either through manual file importation, or automated electronic interface with law enforcement agencies in other jurisdictions (including the United States of America, the United Kingdom, Canada, Jamaica, as well as Interpol.)

10.1.6 Tenderer may optionally provide information on their proposed solution's ability to integrate with other systems, including booking systems, criminal records management systems, and jail management systems.

11. Warranty / Support Requirements

11.1.1 Equipment that will be owned by the RCIPS shall be delivered with a minimum of a one-year warranty for all defects not caused by abuse as judged by the RCIPS. Warranty term shall begin upon acceptance of the solution by the RCIPS. Other potential equipment ownership models shall be entertained and reviewed by the RCIPS.

11.1.2 The Tenderer shall provide detailed pricing for hardware and software maintenance for each year of the four years following the warranty period.

11.1.3 The Tenderer's maintenance support plan shall include 24/7 phone and email support in their offer.

11.1.4 The Tenderer's warranty and maintenance support shall include one central contact point for all hardware and software covered in the proposal. The system availability as measured by system performing as noted in requirements, including availability to operators with searches operational, shall meet or exceed 99% for 8760 hours per year.

11.1.5 The Tenderer shall have the ability to provide onsite support in the Cayman Islands, and shall provide in their proposal their standard hourly rates and terms for such support.

12. Training Requirements

12.1.1 The Tenderer shall provide onsite "Train the Trainer" training for up to five (5) RCIPS or other Cayman Islands Government staff covering the use, administration, and care of the system and its components. Such training shall enable the RCIPS trained staff to provide training to other RCIPS staff as required.

12.1.2 The Tenderer shall supply the following materials for the purposes of training staff:

12.1.2.1 Physical and electronic copies of system manuals and user guides; and

12.1.2.2 Editable electronic copies of the system training materials.

13. **Acceptance Requirements**

At the commencement of the project, the Tenderer shall provide an acceptance test plan to the RCIPS. The following requirements, at a minimum, shall be included in the acceptance plan:

13.1 A process for requirements verification testing, including:

13.1.1 Methodologies for performing acceptance testing against all solution requirements (e.g., test, observation, analysis); and

13.1.2 An estimate of the time required for testing.

13.1.3 A verification process for any hardware supplied.

13.1.4 A verification process for any data migration performed.

13.1.5 A verification process for accuracy of the system.

13.1.6 A verification process for throughput of the system.

14. Optional - Mobile AFIS Device Requirements

14.1 Tenderer's may propose and provide detailed pricing on the provision of Mobile AFIS devices to support the RCIPS' law enforcement activities. Mobile AFIS devices must be integrated with upgraded AFIS infrastructure and must comply with detailed requirements below.

14.2 The Mobile AFIS device should allow the RCIPS to:

14.2.1 Capture and submit fingerprint information to the AFIS system remotely;

14.2.2 Capture and submit latent fingerprints to the AFIS system remotely; and

14.2.3 Perform searches against the AFIS system using captured fingerprint data, and view results of those searches, including linked information from the CMS.

14.3 The Mobile AFIS device shall use an optical fingerprint reader.

14.4 The Mobile AFIS device shall support one or more of the following wireless communication protocols:

14.4.1 A cellular communications protocol (e.g. GPRS/EDGE) offered by providers in the Cayman Islands (e.g. a local cellular company such as LIME or Digicel). This requirement can be met by providing a device that does not have internal cellular support but can access cellular communications by operating with a RIM BlackBerry device in tethered mode. Tenderers shall provide details of supported device(s) (including required device software revision levels) and any third party software required.

14.4.2 Wi-Fi (802.11g or higher).

14.5 The Mobile AFIS device shall support TCP/IP communication, either via wired Ethernet (100 Mbps or higher) or secure Wi-Fi (802.11g or higher).

14.6 The Mobile AFIS device shall have the ability to encrypt data transmissions to protect against interception using industry standard encryption.

14.7 The Tenderer shall specify the encryption algorithm and key size used by their Mobile AFIS device.

14.8 The Tenderer shall not propose proprietary encryption schemes.

14.9 The Mobile AFIS device shall have the ability to confirm successful receipt of transmissions by the back-end system, and to retransmit in the event of transmission failure.

14.10 The Mobile AFIS device shall have the ability to securely receive and decrypt responses of a search and to display this information to the RCIPS enforcement officer.

14.11 The Mobile AFIS device shall have the ability to internally store a repository of up to 20,000 (twenty thousand) biometric records.

14.12 These records shall include the subject's first name, last name, at least two fingerprint images, and facial image. It is estimated that each record will consume no more than 500 Kilobytes.

14.13 The Mobile AFIS device shall protect the internal repository from unauthorized access.

14.13.1 Tenderer shall explain in detail how the internal repository is protected on their device. The use of encryption for this purpose is preferred.

14.14 In the event that verification queries cannot be sent to the back-end system (e.g., if the Mobile AFIS device is outside of the cellular service area), the device shall have the ability to search the local repository.

14.15 The Mobile AFIS device shall use the biometric data to display a list of candidate matches to the RCIPS enforcement officer.

14.16 The Mobile AFIS device shall the retrieve the subject's name, date of birth and facial image, and to display this information to the RCIPS enforcement officer.

14.17 The Mobile AFIS device shall complete local search requests in no more than 2 minutes.

14.18 The Tenderer shall provide costs for the Mobile AFIS device, including matching software, system software, communications software, and any other required licences.

14.19 Unless otherwise specified in the Tenderer's proposal, licenses shall be assumed to be based solely on the number of Mobile AFIS device units purchased.

14.20 Licenses shall be transferable between Mobile AFIS device without additional charge.

14.21 The Mobile AFIS device shall be capable of operating for at least eight (8) hours on a single battery charge.

14.22 The Mobile AFIS Device battery shall not degrade in performance if recharged before being fully discharged.

14.23 The Mobile AFIS device shall support hot-swap of batteries; i.e., it must be possible to change batteries in the middle of an operation without loss of data.

14.24 Each Mobile AFIS device shall be provided with charger(s) that allow at least two batteries to be charged concurrently.

14.25 Mobile AFIS device chargers must be compatible with 120 VAC, 60 Hz electrical power.

14.26 Each Mobile AFIS device shall be capable of being powered by standard automobile power outlets, either through a dedicated charger or the use of an inverter. Dedicated chargers or compatible inverters, if required, shall be included in the price of the units.

14.27 The Mobile AFIS device shall be capable of operating in temperatures ranging from 35 to 120 degrees Fahrenheit, and relative humidity ranging from 10 to 90%, non-condensing.

14.28 The Mobile AFIS device shall be water resistant; it shall not fail when exposed to rain, or to brief immersion in water.

14.29 The Mobile AFIS device fingerprint scanner shall operate in direct sunlight or shade.

14.30 The Mobile AFIS device shall weigh no more than 4 pounds.

15. Optional – Offsite Disaster Recovery

15.1 Tenderer's may optionally propose and provide detailed pricing on the provision of an offsite disaster recovery solution, to allow storage and access to AFIS and CMS mugshot records in a secure controlled location.

15.2 This option shall be separately priced in the Tenderer's proposal, with the pricing to include all associated costs, including ongoing maintenance, with the option.

15.3 The Tenderer shall specify in their proposal a suggested backup plan for replicating data off-island, including the frequency of backups, type of backups (e.g. full, incremental, etc.) and the approximate network bandwidth requirements to meet the plan.

Parts A & B

Acceptance Criteria

Tenderer shall include in their tender a proposed approach to verifying that their offer meets the specified requirements. The Government reserves the right to negotiate modifications to the Tenderers' proposed acceptance criteria to ensure compliance with all requirements. At a minimum, the acceptance criteria should include, an inventory of the provided software and hardware (including licence keys), documented methods to validate that the Hardware and Software meet the specified requirements, and successful demonstration of the Hardware and Software operating consistent with the specified requirements.

Execution of Contract

The successful Tenderer shall be required to execute a contract in the terms as agreed between the parties. Tenderers must ensure they understand the completeness of the information and documentation required to be provided when submitting a proposal. There is no obligation on the Department to request additional information during the proposal evaluation stage.

Project Timetable

The tentative timetable for this project is as follows. All times and dates are local Cayman time.

1. Invitation to Tender released:8th October, 2010
2. Deadline for queries on the tender: Noon, 8th November, 2010
3. Deadline for return of proposals: Noon, 19th November, 2010
4. Evaluation of proposals: 19th November, 2010 – 01st December, 2010
5. Notification to successful Tenderer/s: After the 5th December, 2010
6. Contract negotiation: (1-2 weeks after Award)
7. Tenderer/s signs contract: (2 weeks after Award)
8. Hardware and Software deliverables due: (6 – 8 weeks after Award)
9. User training completed: (8 – 10 weeks after Award)

10. Hardware and Software Acceptance Testing: (10 – 15 weeks after Award)

11. Final Hardware and Software Acceptance Sign-Off: (16 weeks after Award)

End of Section 3: Conditions of Tender.

SECTION 4: ASSESSMENT CRITERIA

All proposals received by the submission deadline will be evaluated by the Portfolio of Internal & External Affairs Immigration Biometric Enrolment, Verification, and Enforcement Hardware and Software, and Law Enforcement Automated Fingerprint Identification System Hardware and Software Project Team on specific weighted criteria as follows:

1. Price (must not exceed budgeted amount of CI $750,000) 30%
2. Proposal Submission (quality and completeness) 5%
3. Experience (equal to or superseding this project) 10%
4. References (previous successful project completion) 10%
5. Ability to meet established project time-table 5%
6. Core requirements (ability to meet section 3 technology, warranty, support and training requirements) 40%

Total 100%

End of Section 4: Assessment Criteria.

TENDER PRICE FORM

This form is mandatory to include with your proposal.

TENDER NO: CTC/10-11/PIE/016

FOR: Immigration Biometric Enrolment, Verification, and Enforcement Hardware and Software, and Law Enforcement Automated Fingerprint Identification System Hardware and Software

SUBMITTED
BY:

_____
(PRINT Name of Person)

FOR AND ON
BEHALF OF:

_____
(PRINT Name of Company)

Company Street Address: _____

Company Postal Address: _____

Company Tel &/or Cell: _____

Contact email address: _____

==========

Part A: Immigration Biometric Enrolment, Verification, and Enforcement Hardware and Software

Enrolment Equipment and Supporting Software	$ _____ Cayman Islands Dollars
Verification Equipment & Supporting Software	$ _____ Cayman Islands Dollars
Single Finger Matching Software Development Kit & License	$ _____ Cayman Islands Dollars
Fingerprint 1:N Uniqueness Search System & License	$ _____ Cayman Islands Dollars
Mobile Fingerprint Capture and 1:1 Matching Device (MFCMD)	$ _____ Cayman Islands Dollars

**TOTAL PROPOSAL $ _____ Cayman Islands Dollars

Year 1 Annual Maintenance: $ _____ Cayman Islands Dollars

Year 2 Annual Maintenance: $ _____ Cayman Islands Dollars

Year 3 Annual Maintenance: $ _____ Cayman Islands Dollars

Year 4 Annual Maintenance: $ _____ Cayman Islands Dollars

Year 5 Annual Maintenance: $ _____ Cayman Islands Dollars

Enrolment Equipment and Supporting Software Year 1 Annual Maintenance: $ _____ Cayman Islands Dollars Year 2 Annual Maintenance: $ _____ Cayman Islands Dollars Year 3 Annual Maintenance: $ _____ Cayman Islands Dollars Year 4 Annual Maintenance: $ _____ Cayman Islands Dollars Year 5 Annual Maintenance: $ _____ Cayman Islands Dollars
Verification Equipment & Supporting Software Year 1 Annual Maintenance: $ _____ Cayman Islands Dollars Year 2 Annual Maintenance: $ _____ Cayman Islands Dollars Year 3 Annual Maintenance: $ _____ Cayman Islands Dollars

Year 4 Annual Maintenance: $ _____ Cayman Islands Dollars Year 5 Annual Maintenance: $ _____ Cayman Islands Dollars
Single Finger Matching Software Development Kit & License Year 1 Annual Maintenance: $ _____ Cayman Islands Dollars Year 2 Annual Maintenance: $ _____ Cayman Islands Dollars Year 3 Annual Maintenance: $ _____ Cayman Islands Dollars Year 4 Annual Maintenance: $ _____ Cayman Islands Dollars Year 5 Annual Maintenance: $ _____ Cayman Islands Dollars
Fingerprint 1:N Uniqueness Search System & License Year 1 Annual Maintenance: $ _____ Cayman Islands Dollars Year 2 Annual Maintenance: $ _____ Cayman Islands Dollars Year 3 Annual Maintenance: $ _____ Cayman Islands Dollars Year 4 Annual Maintenance: $ _____ Cayman Islands Dollars Year 5 Annual Maintenance: $ _____ Cayman Islands Dollars
Mobile Fingerprint Capture and 1:1 Matching Device (MFCMD) Year 1 Annual Maintenance: $ _____ Cayman Islands Dollars Year 2 Annual Maintenance: $ _____ Cayman Islands Dollars Year 3 Annual Maintenance: $ _____ Cayman Islands Dollars Year 4 Annual Maintenance: $ _____ Cayman Islands Dollars Year 5 Annual Maintenance: $ _____ Cayman Islands Dollars

Part B: Automated Fingerprint Identification System Hardware and Software.

AFIS Equipment and Supporting Software	$ _____ Cayman Islands Dollars
Desktop/Portable Livescan Terminals	$ _____ Cayman Islands Dollars
Optional: Mobile AFIS Devices	$ _____ Cayman Islands Dollars
Optional: Offsite Backup / DR Solution	$ _____ Cayman Islands Dollars

**TOTAL PROPOSAL $ _____ Cayman Islands Dollars

Year 1 Annual Maintenance: $ _____ Cayman Islands Dollars

Year 2 Annual Maintenance: $ _____ Cayman Islands Dollars

Year 3 Annual Maintenance: $ _____ Cayman Islands Dollars

Year 4 Annual Maintenance: $ _____ Cayman Islands Dollars

Year 5 Annual Maintenance: $ _____ Cayman Islands Dollars

AFIS Equipment and Supporting Software Year 1 Annual Maintenance: $ _____ Cayman Islands Dollars Year 2 Annual Maintenance: $ _____ Cayman Islands Dollars Year 3 Annual Maintenance: $ _____ Cayman Islands Dollars Year 4 Annual Maintenance: $ _____ Cayman Islands Dollars Year 5 Annual Maintenance: $ _____ Cayman Islands Dollars
Desktop/Portable Livescan Terminals Year 1 Annual Maintenance: $ _____ Cayman Islands Dollars Year 2 Annual Maintenance: $ _____ Cayman Islands Dollars Year 3 Annual Maintenance: $ _____ Cayman Islands Dollars Year 4 Annual Maintenance: $ _____ Cayman Islands Dollars Year 5 Annual Maintenance: $ _____ Cayman Islands Dollars
Optional: Mobile AFIS device Year 1 Annual Maintenance: $ _____ Cayman Islands Dollars Year 2 Annual Maintenance: $ _____ Cayman Islands Dollars

Year 3 Annual Maintenance: $ _____ Cayman Islands Dollars Year 4 Annual Maintenance: $ _____ Cayman Islands Dollars Year 5 Annual Maintenance: $ _____ Cayman Islands Dollars
Optional: Offsite Backup / DR solution Year 1 Annual Usage/Maintenance: $ _____ Cayman Islands Dollars Year 2 Annual Usage/Maintenance: $ _____ Cayman Islands Dollars Year 3 Annual Usage/Maintenance: $ _____ Cayman Islands Dollars Year 4 Annual Usage/Maintenance: $ _____ Cayman Islands Dollars Year 5 Annual Usage/Maintenance: $ _____ Cayman Islands Dollars

End of Document.